Windows Privacy Update

Jeffrey Friedberg
Director of Windows Privacy

Agenda

- New Home
- XP-SP2
- Deceptive Software
- Phishing
- Q & A

Now in SBTU

- Better synergy
  - Teams share similar strategies and general processes
- Reduce tax on developers
  - Integrate privacy into Security Development Lifecycle
- More efficiently work critical projects
  - Tap combined expertise
  - Better way to address issues like deceptive software and phishing that cross domains

Structure and Focus

- Organization
  - JeffreyE coordinating WPI
  - Privacy Cabinet and Leads unchanged
- Short Term
  - Complete XP SP2
  - Drive Longhorn Privacy Basic
- Long Term
  - Integrate privacy with SDL

XP-SP2 Privacy Disclosures

- Posted final statements for Windows and IE
  - *First time these existed for Microsoft!*
  - Huge effort – lots of material, many teams
- Setting up a web-based feedback channel
  - Need to cut the Spam
  - Stop gap until MPRC
- Ad hoc international support
  - Localizing feedback pages
  - Internal groups on call to translate

Deceptive Software

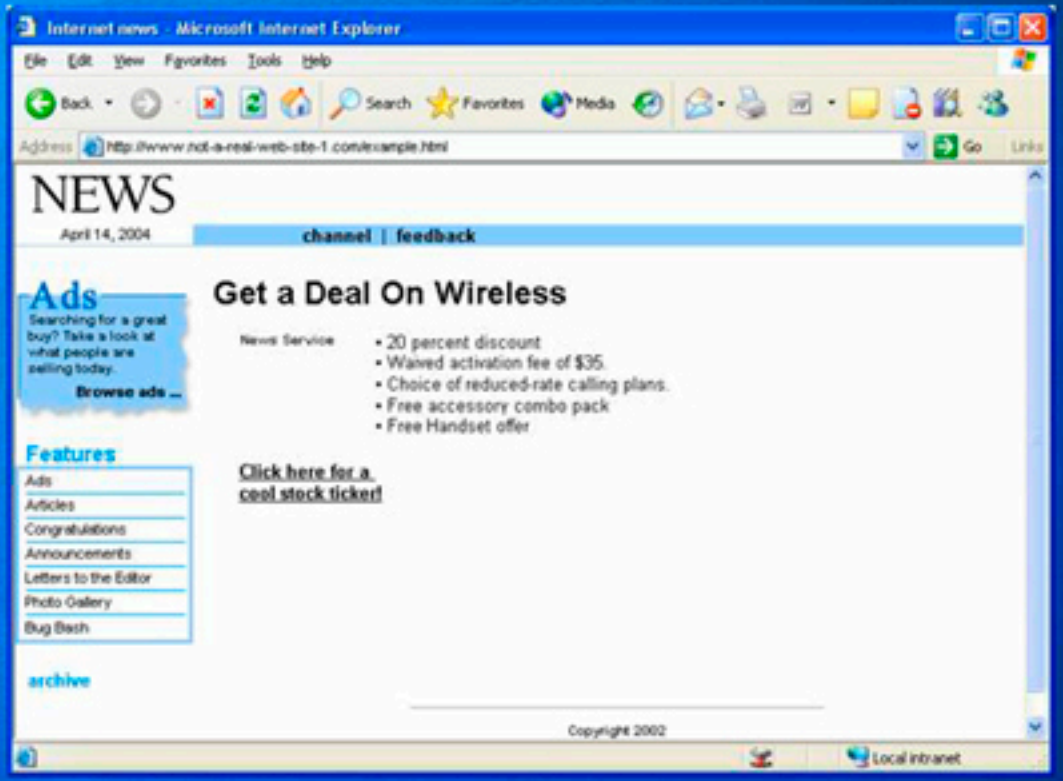
Examples, Strategy, and Best Practices

What is Deceptive Software?

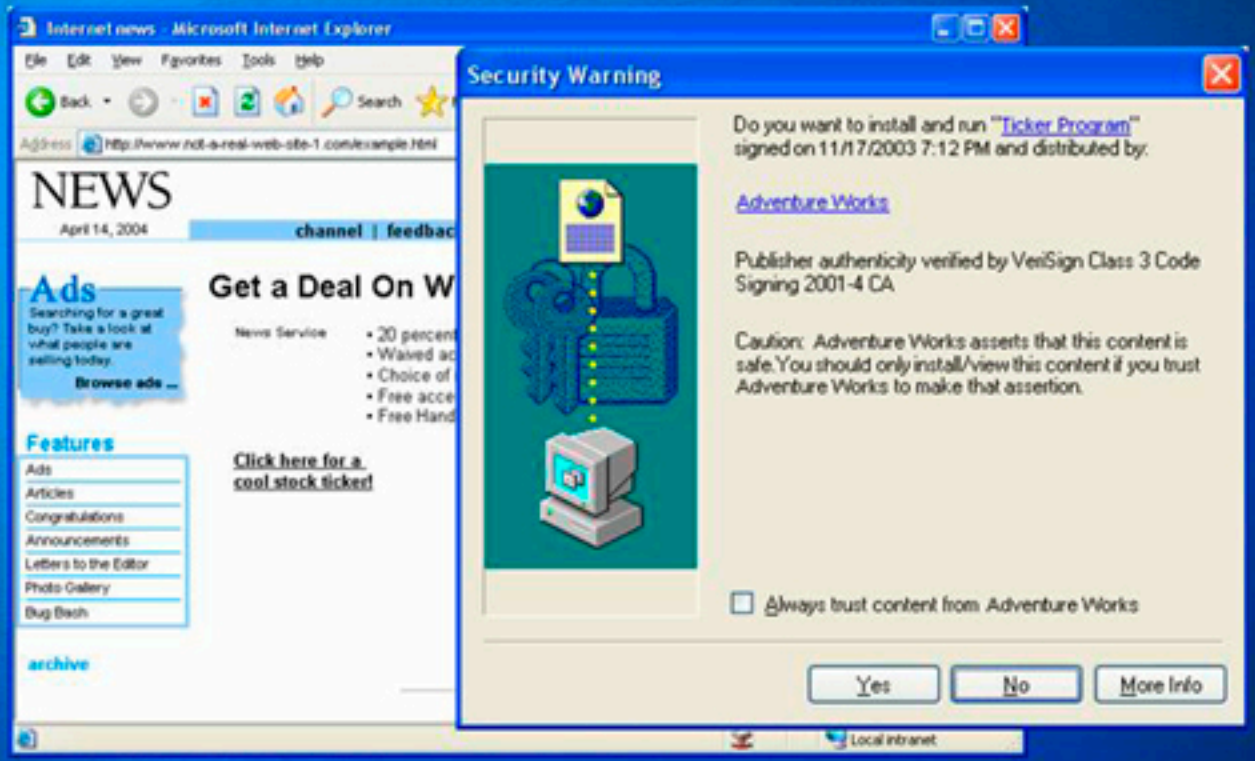
- Includes spyware and its variants:
  - Unauthorized adware, browser hijackers, dialers
- Common theme: use of deception
  - Users often tricked and/or unaware
  - Difficult uninstalls and sneaky reinstalls
- Customers frustrated, feel out of control
  - Systems can become unusable
- With proper consent features can be desirable
  - Personalization, reduced cost, better experience

Normal Download Experience

User Initiates Download

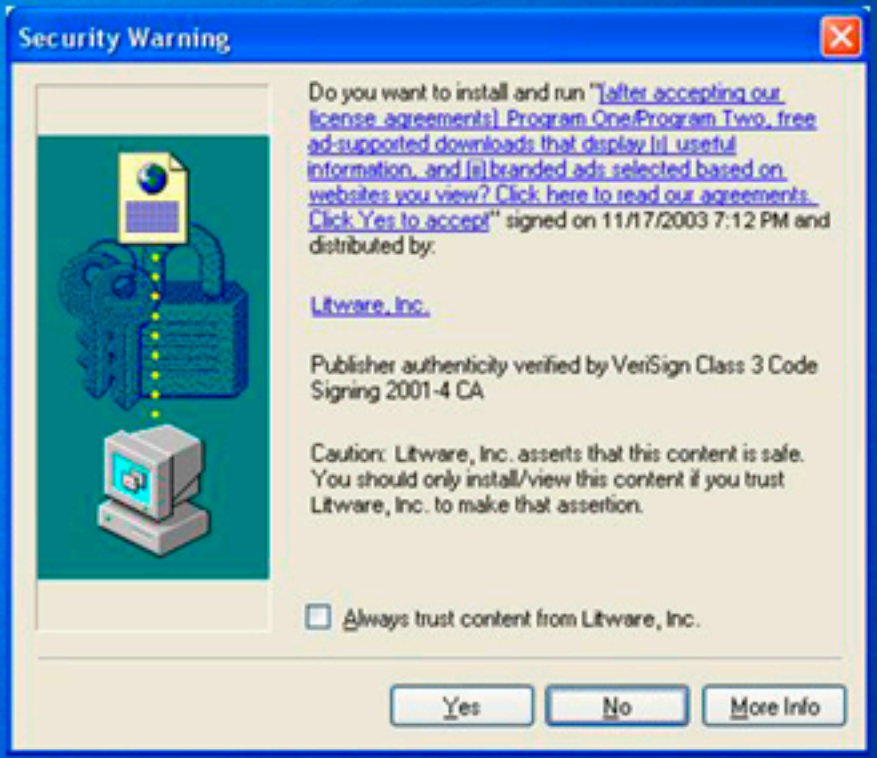


Security Warning Displayed



Some Common Tricks

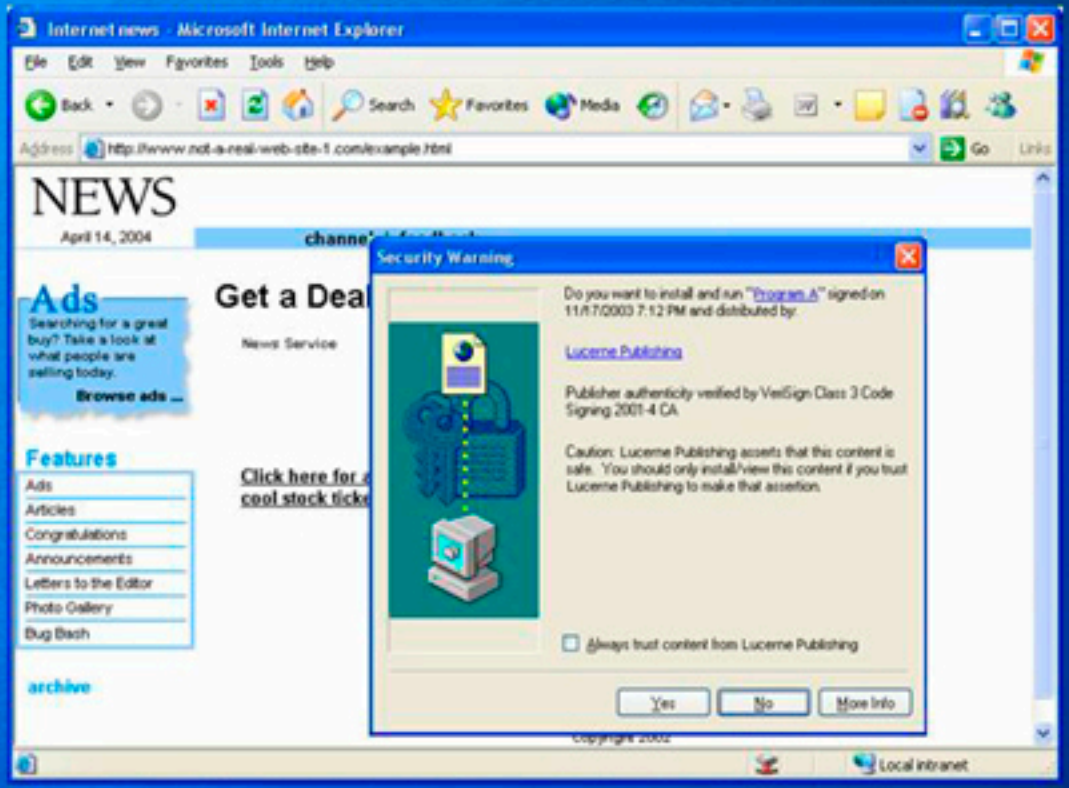
Multi-line Program Name



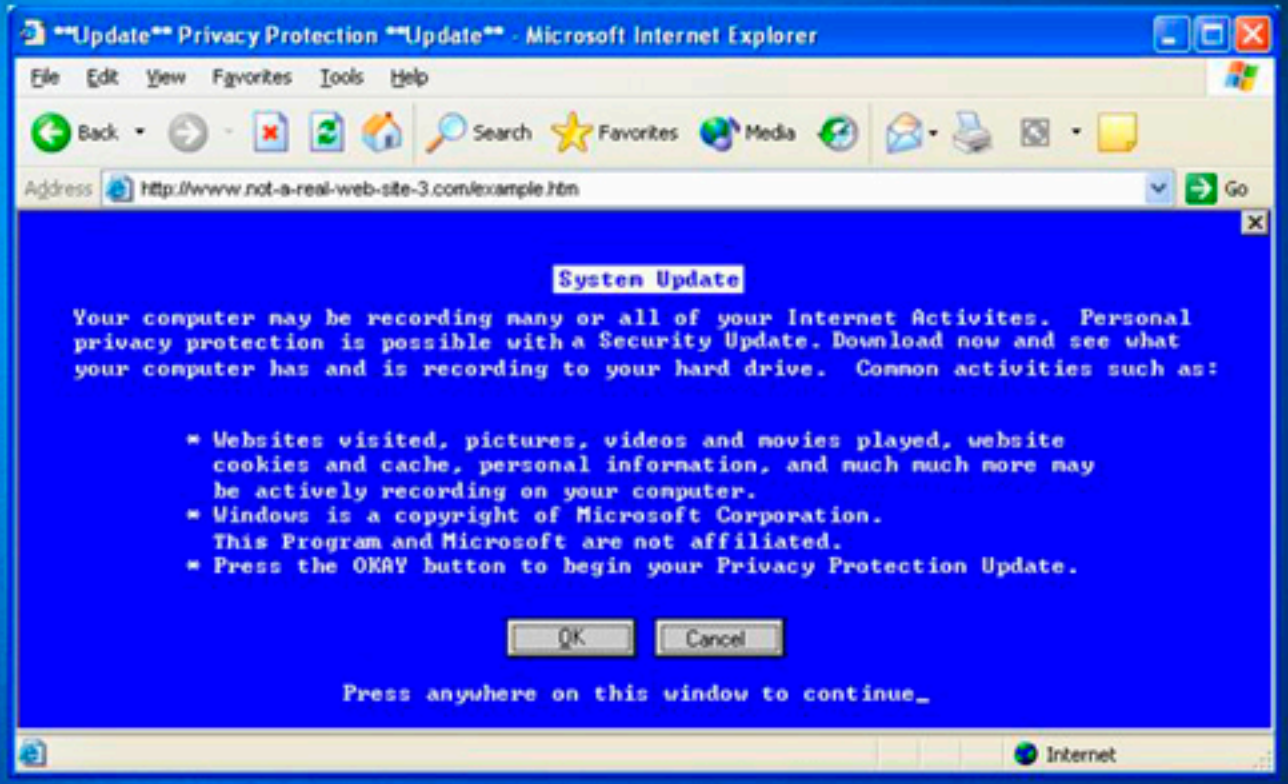
EULA Detail

- **UPDATES.** You grant Litware permission to add/remove features and/or functions to the existing software and/or service, or to ***install new applications, at any time,*** in its sole discretion with or ***without your knowledge*** and/or interaction. By doing so, ***you agree to the terms of the new applications.*** You also grant Litware permission to make any changes to the software and/or service provided at any time.

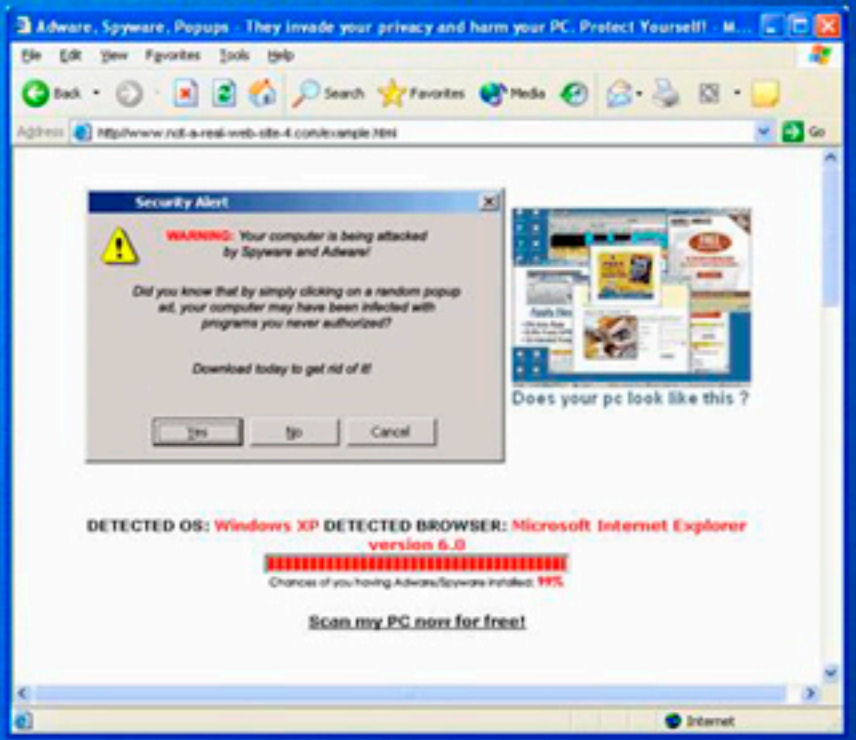
Pop-Under Exploit



“Cancel” Means “Yes”



Faux Security Alert
(really just a picture)

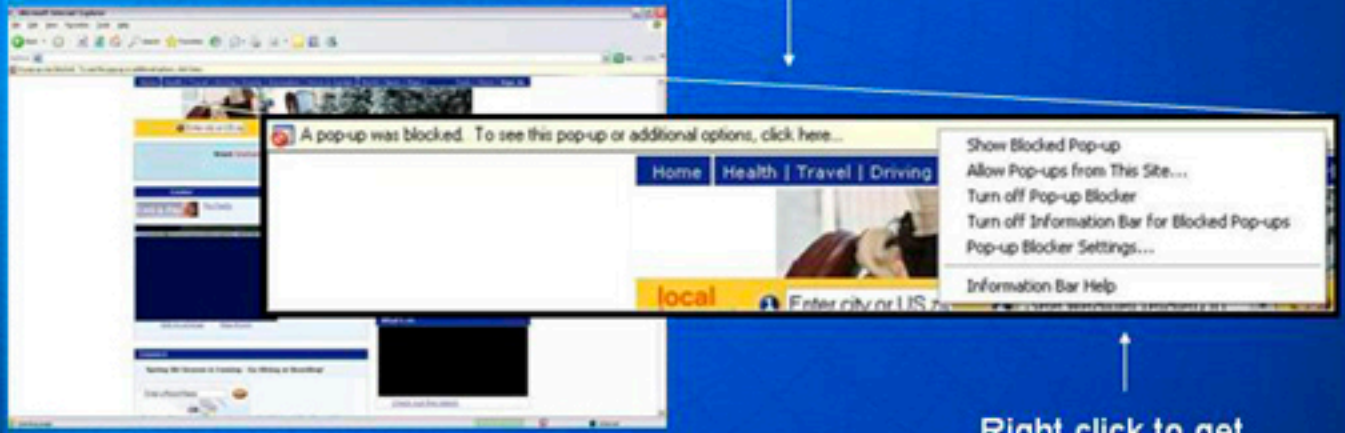


Don’t Leave Your Front Door Open

Some XP SP2 Enhancements that Help Address the Problem

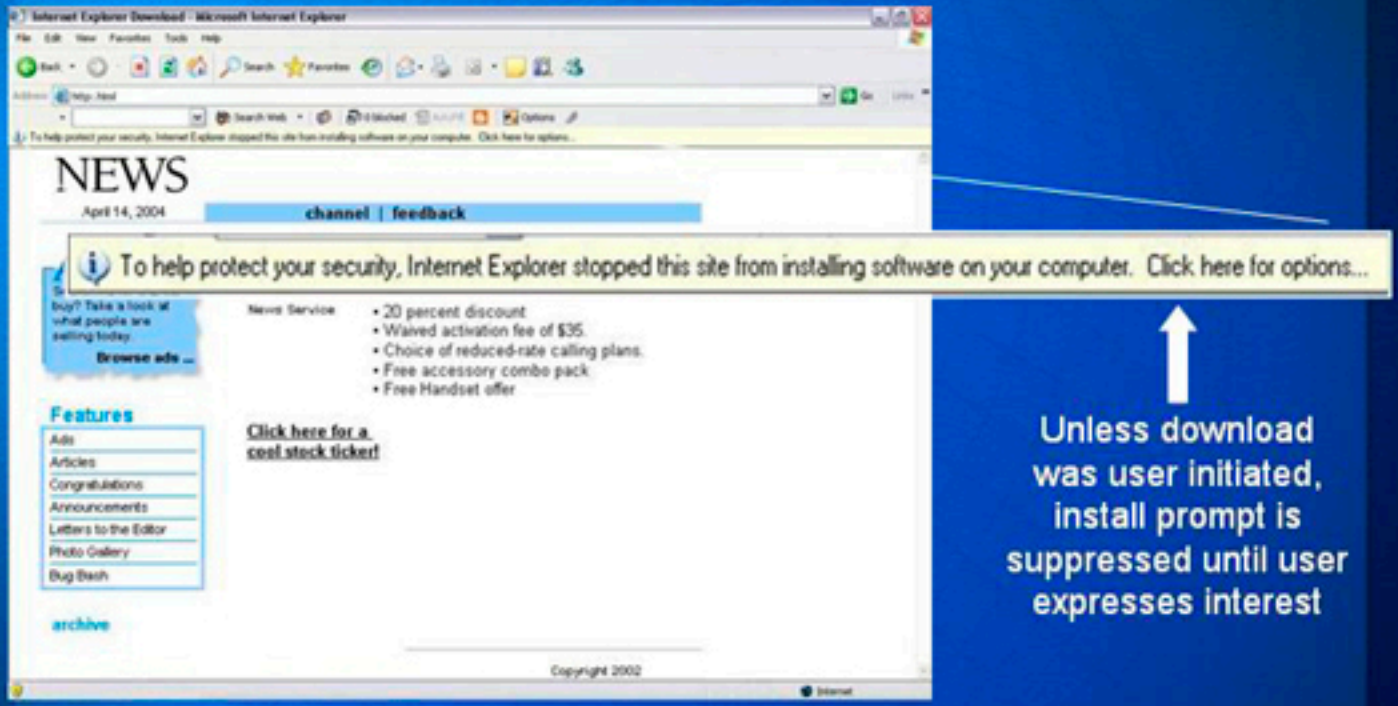
New Popup Blocker

Information Bar provides
Notice and Choice



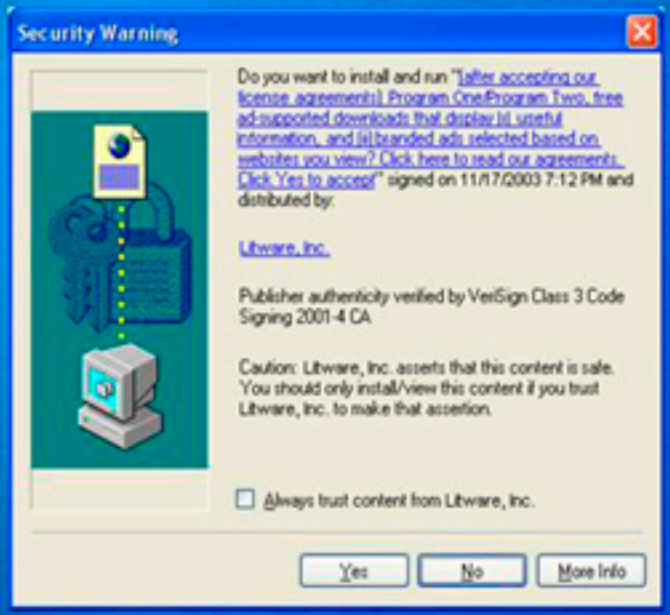
Right click to get
more options

New Download Blocker



Unless download was user initiated, install prompt is suppressed until user expresses interest

Improved Install Prompts



Current

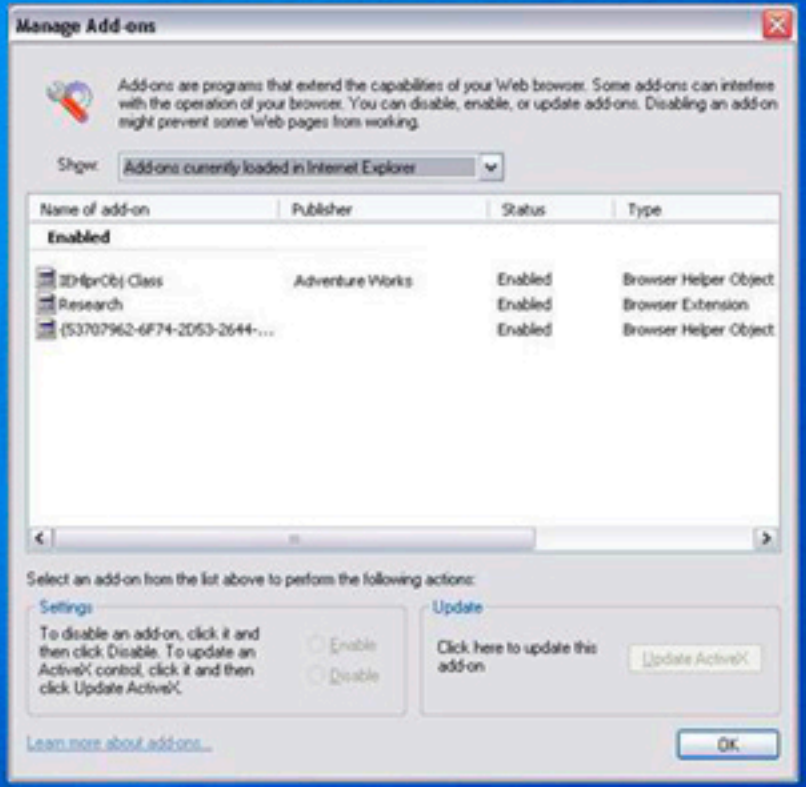
Cannot overload text fields

New

Can choose "Never Install"

Harder to Leave Your Front Door Open

New Add-on Manager



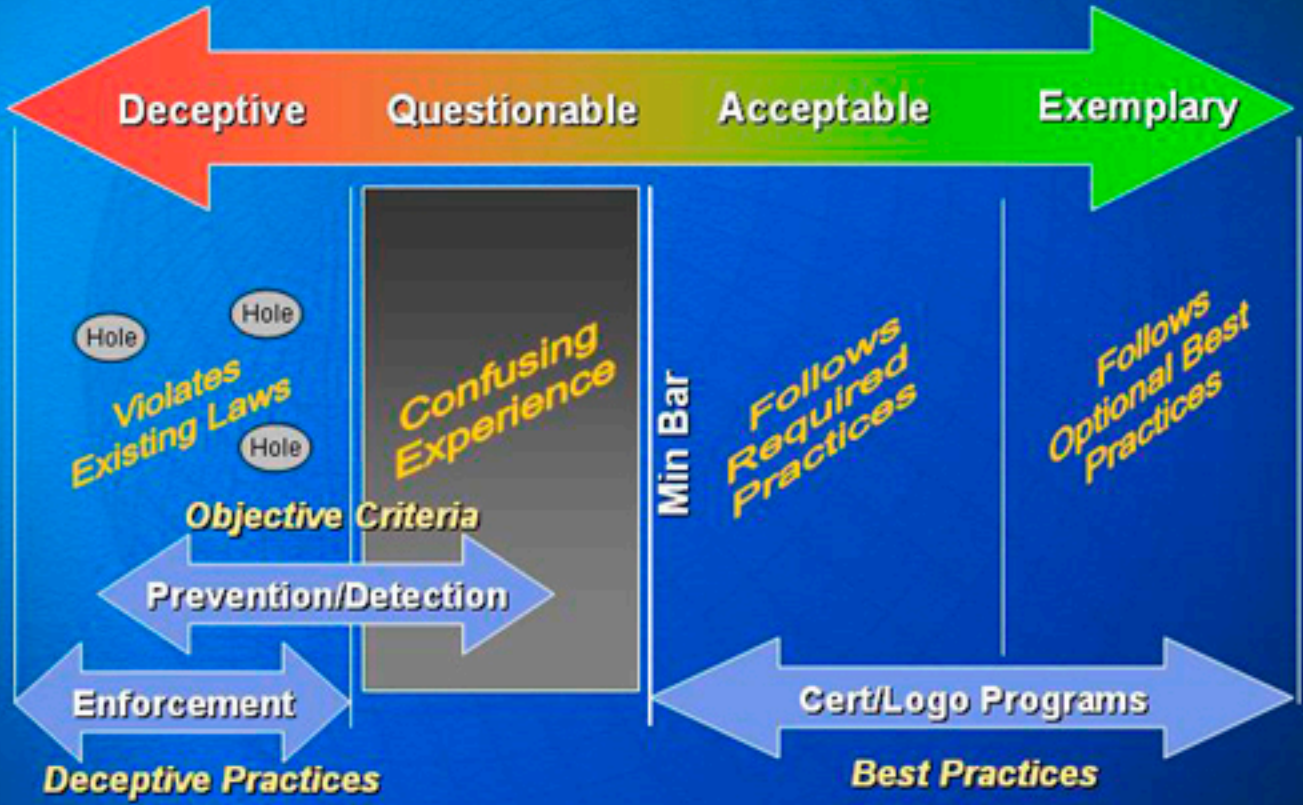
User can Enable/Disable ActiveX Controls and Browser Helper Objects (e.g. Toolbars)

Neutralize unwanted software

Pursuing Holistic Strategy

- Consumer Education
  - Launched www.microsoft.com/spyware portal
- Technology Investments
  - Releasing enhancements in XP SP2
- Industry Cooperation
  - Identified Best Practices (key to self regulation)
  - Active in CDT Working Group
- Enforcement Deterrent
  - Engaged FTC (workshop and investigations)
- Legislation - as needed
  - Focus on bad behavior not software features

Range of Behaviors



Best Practices

- Under development since November
- Vetted with Windows, Office, MSN, CPG
- Completed executive review
- Minor house cleaning
- Ready to engage

Scope

- Share personal data or surfing behavior
- Display ads in distinct user experience
- Change configuration settings that substantially alter desktop experience

Range of Compliance

- Required Practices
  - Must be followed
  - Fail to meet risk being labeled deceptive or illegal
- Recommended Practices
  - Would increase transparency and control
  - Should be followed unless compelling technical, security, or business reason not to do so

End User Trust Catchall

- Avoid features that:
  - Are provided for direct personal financial gain of somebody other than the user with no compelling direct user value in return
  - Could be construed as offensive by typical user
  - Disrupt a user's desktop experience

Notice and Consent

- Prominent versus discoverable
  - Substantive aspects above the fold
  - Intelligent summary with link to details
  - Challenge with EULA's
- Consent
  - Additional action based on sensitivity
  - Fill in the blank OK

Information Sharing

- For personal data or surfing behavior:
  - Prominent notice and consent experience required prior to execution
  - Discoverable notice recommended prior to installation of software
- For anonymous data:
  - Discoverable notice recommended prior to execution

Advertisement Display

- For "standalone" ads:
  - Prominent notice and consent experience required prior to installation
  - Attribution and easy to discover and use control mechanism also required
- For "embedded" ads:
  - No special notice, consent, or control

Configuration Changes

- For those that substantially alter desktop experience:
  - Prominent notice and consent experience required prior to execution

Disable and Uninstall

- Mechanism to disable and completely uninstall recommended, unless …
- Prominent notice and consent experience required prior to installation if mechanism not provided

Phishing

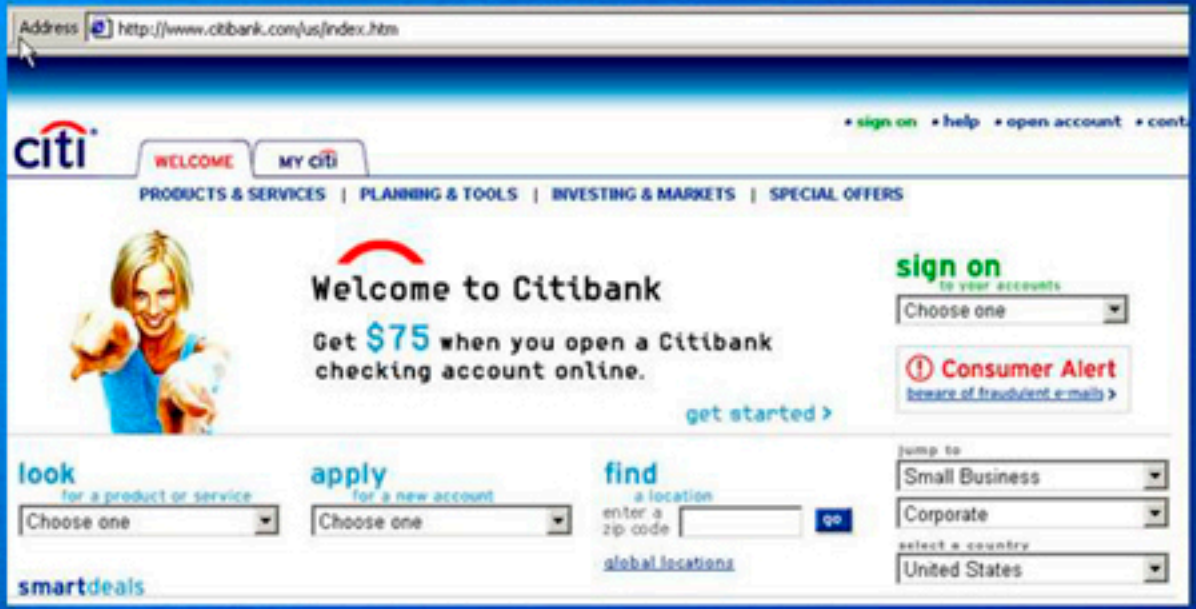
Vision, Strategy, Tactics

External Situation

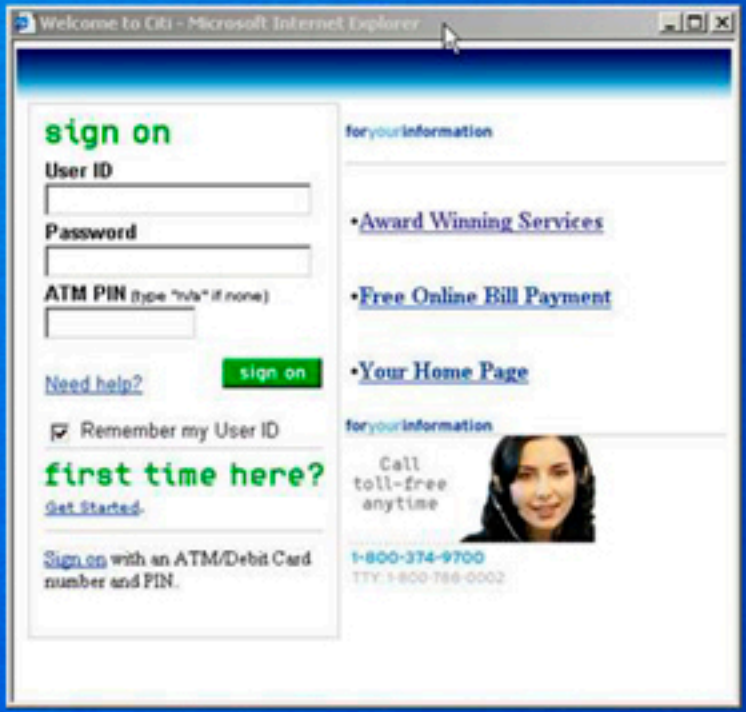
- Many falling for scams
  - 2M in 2003 (57M attempts)
- Tricks getting more elaborate
  - Multiple emails, blended threats
- Technology cannot solve everything
  - Some users just too trusting
- Phishing is profitable
  - Economics favor the bad guys
- Real concern for eCommerce
  - $2B in losses last year
- Financial partners want action
  - Want to know our roadmap

Get Email from a Spoofed Sender with a Spoofed Link

Fake Site Immediately Redirects to Trusted Site



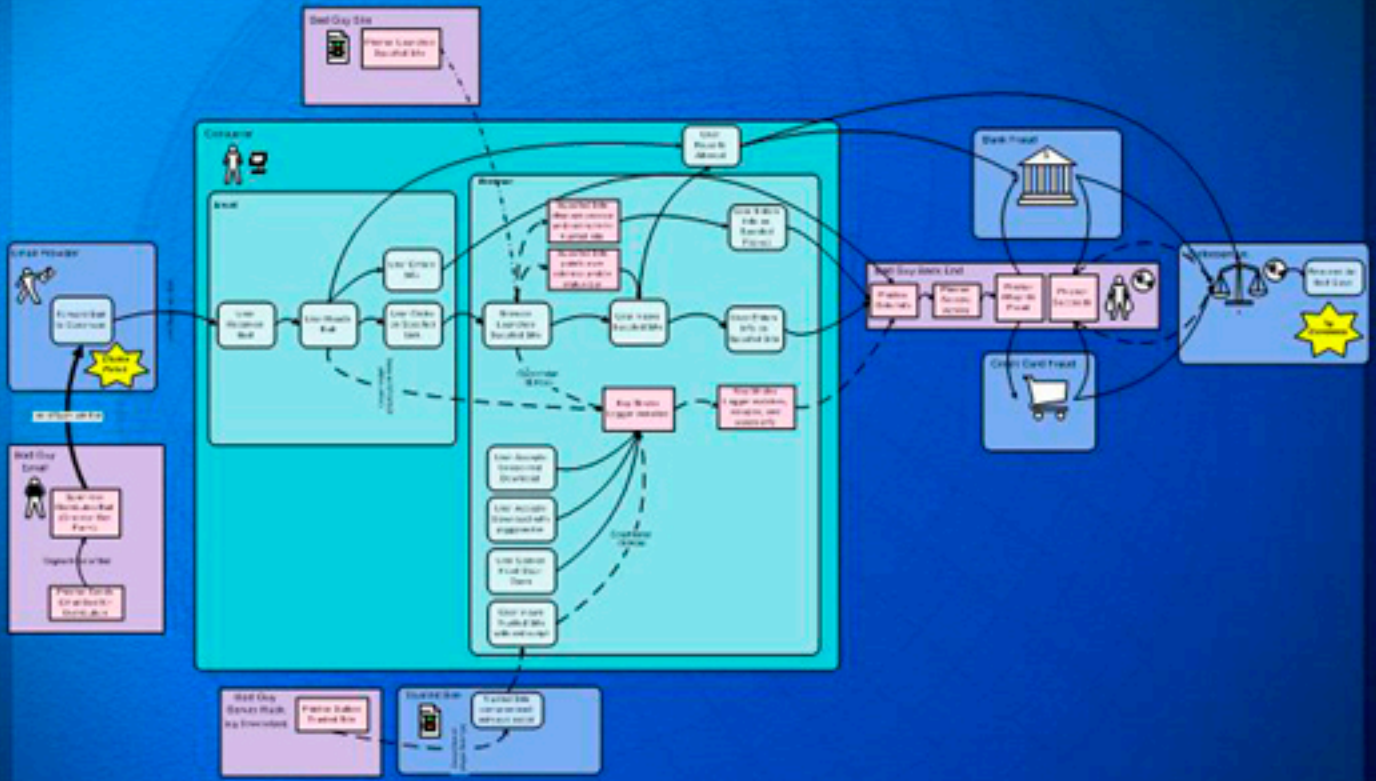
User Gets Fake Pop-up Window With No URL to Tip Them Off!



Internal Situation

- Many independent internal efforts
  - Anti-Spam (Safety), MSN, IE, Outlook, Security, LCA, Project Protect, …
  - Some tactical, some strategic
- Asked by SBTU management to lead Phishing Task Force
  - Coordinate company-wide activities
  - Establish longer-term unified roadmap
  - Reduce overlap, spot and fill holes in strategy
- Launched task force on 6/15

Phishing Battlefield



Vision

Windows customers are safe from electronic fraud while using the Internet

Strategy

Before an Attack	*During an Attack*	*After an Attack*
Reduce Attack Volume	Make it easy to validate email	Make it easy to report
Reduce Covert Attacks	Make it easy to validate a site	Collect and Analyze tricks
Reduce Attack Impact	Make it easy to tell if I'm being watched	Identify ways to prevent or avoid
Protect Critical URLs		Create deterrents through enforcement
Ensure Visual Integrity		
Increase User Awareness		

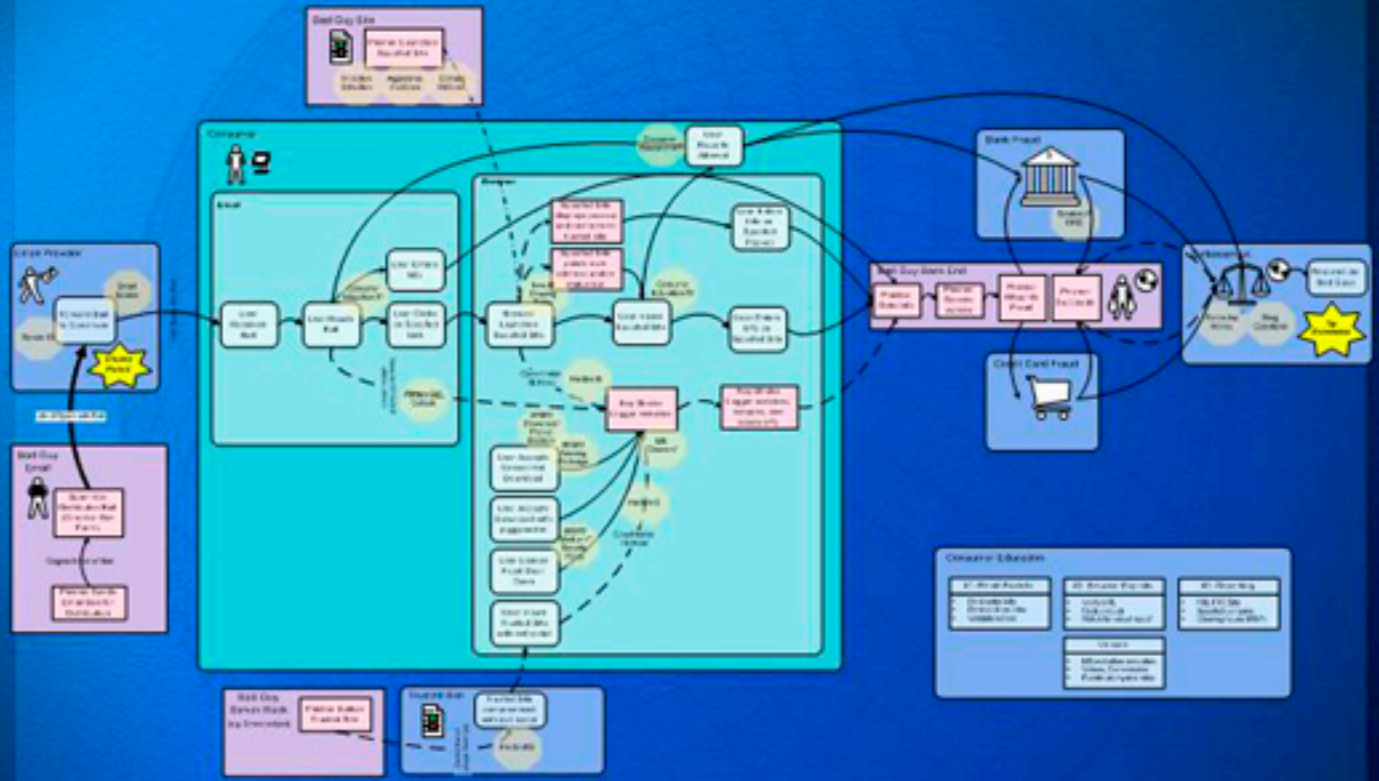
Tactics in Play Now

- Smart Screen (2.7B messages blocked per day)
- Online consumer education
- Proactive detection of spoofed sites, aggressive shutdown, domain defense
- "Follow the money" enforcement
- Cleaner for Download.ject key stroke logger
- Fixes for known vulnerabilities
- Scratch off PINs (low tech bank solution)

Tactics About to be Deployed

- XP SP2 mitigations (Aug)
- "Phishnet" Sting Operation (Aug)
- Education through Project Protect (Fall?)
- Sender ID (Now - Oct)

Battlefield Tactics – Short Term View



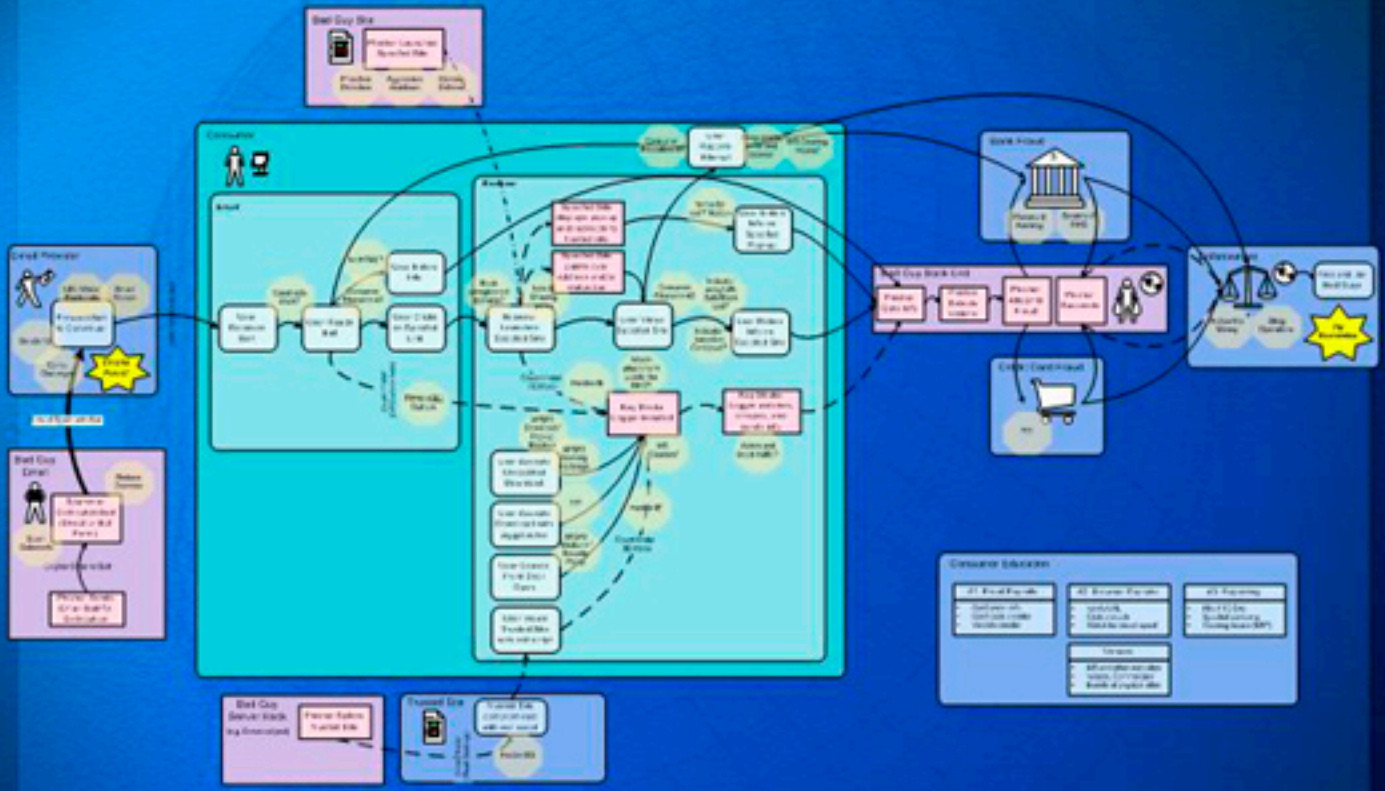
Tactics in the Queue

- Add URL safe/block list to Smart Screen
  - Investigating 3rd party aggregator
- Add UI to report an email fraud
  - Hotmail 3.0?

Other Tactics Being Discussed

- Add URL safe/block list to browser
- Add "report a suspected site" to browser
- Detect and block unregistered domains
- Add computational challenges
- Detect and block zombies
- Detect and block of key stroke loggers
- Watch browser attachment points (add-ons)
- Add password hashing
- Increase visual integrity

Battlefield Tactics – Long Term View



Next Step – Optimize Investments

- Establish end to end plan that provides best coverage over time for the worst harms
  - Consider consumers, partners, and our reputation
  - Assess status of current and proposed tactics
    - Identity owner, schedule, release vehicle, risks, issues
    - Gauge efficacy relative to harms
  - Identity holes, improvements
- Get plan approved and execute
  - Refocus projects as needed
  - Help teams acquire resources and go

Q&A

Reference Materials

- XP-SP2 Windows Privacy Statement
  - http://www.microsoft.com/windowsxp/downloads/updates/sp2/docs/privacy.mspx
- XP-SP2 IE Privacy Statement
  - http://www.microsoft.com/windowsxp/downloads/updates/sp2/docs/privacy_ie.mspx
- Consumer Education Sites
  - http://www.microsoft.com/phishing
  - http://www.microsoft.com/spyware